SECTION 1. GENERAL

1.1 Purpose. This is a guide for the Standard Army Retail Supply System-Gateway (SARSS-GW) system manager at the installation, corps, theater or state level. This manual defines procedures the system manager uses to manage the SARSS-GW.

NOTE: The SARSS Gateway was originally named Objective Supply Capability (OSC) and is now called the SARSS-GW. All references to OSC and gateway have been changed or refer to SARSS-GW.

1.2 References. See appendix A for documents that form parts of this manual. If this manual is in conflict with a regulation, report such conflicts (see paragraph 1.5). Until resolution of the conflict, follow the regulation. If following the regulation causes disruption, follow the manual.

1.3 Terms and Abbreviations. See appendix B for terms, abbreviations, and acronyms used in this manual.

1.4 Security. Commanders and managers are responsible for physical, personal, communication, software, hardware, and procedural security in their own data processing operations. Army Regulation (AR) 380-19 contains detailed instructions concerning responsibilities, policies, procedures, and guidance for automated systems security.

1.4.1 System Access. No classified, personal, or proprietary data is processed by the SARSS-GW. Log-in identification (ID) and password controls are required by the defense information service network (DISN) and the SARSS-GW. The information systems security officer (ISSO), together with the system manager, controls and issues log-in IDs, passwords, and Access Codes. System access must be granted to each standard Army management information system (STAMIS) user, supply and resource manager, and the system manager. (See appendix C for access information.)

1.4.2 SARSS-GW Application. SARSS-GW's database and programming logic reside on a computer at a central location. The computer is linked to SARSS-GW users and supporting supply activities using modems and/or LAN connections. The SARSS-GW host and the SARSS-GW database administrator (DBA) are responsible for security and site management.

1.4.3 Army Installations. The ISSO and the terminal area security officer (TASO) are responsible for developing physical and informational security plans. These plans must prevent unauthorized access to systems that connect to the SARSS-GW.

1.5 Proponent Statement. The United States Army Information Systems Software Development Center, Lee (USAISSDCL) is the proponent agency (PA). Recommended changes and comments for this publication may be submitted on DA Form 2028 and sent to:

USAISSDCL DSD DIV A L32
ATTN AMSEL SE IS SDL SA
3901 C AVE SUITE 150
FORT LEE VA 23801-1807